Elliptical Curve Digital Signatures Algorithm

Prajna. D
Student (Mtech) of Dept of Digital electronics
UTL tech limited
Bangalore, 560012, India
Prajna.dayalan@gmail.com

Prof. Mrs. Leelavathi
UTL Tech limited
Bangalore, India.
Nisargamodini@gmail.com

Abstract- Elliptical digital signatures algorithm provides security services for resource constrained embedded devices. The ECDSA level security can be enhanced by several parameters as parameter key size and the security level of ECDSA elementary modules such as hash function, elliptic curve point multiplication on koblitz curve which is used to compute public key and a pseudo-random generator which generates key pair generation. This paper describes novel security approach on authentication schemes as a modification of ECDSA scheme.

This paper provides a comprehensive survey of recent developments on elliptic curve digital signatures approaches. The survey of ECDSA involves major issues like security of cryptosystem, RFID-tag authentication, Montgomery multiplication over binary fields, Scaling techniques, Signature generation ,signature verification, point addition and point doubling of the different coordinate system and classification.

Index terms- *Random generator, secure hash algorithm, Elliptic Curve digital signature algorithm. Koblitz curves, FPGA and cryptography.*

*****

I. INTRODUCTION

With the development of information technology and extensive application of information equipment, information security has become the key of dominating nation and society. Digital signatures is one of the technique which provides information security. It play an important role in the communication networks by allowing message integrity, and non-repudiation during transmission over an insecure network. A digital signature scheme is a mathematical scheme which usually demonstrates an authenticity of a digital message. A valid digital signatures gives a recipient reason that the message is generated by the user and it's not modified other than sender. A digital signature is dependent on secret key which is only known to signer (Private Key).and the contents of being message signed. Signatures has to be verified such that if any dispute arises whether an entity signed document, a third party must be able to resolve matter without accessing the private key. Disputes may arise when a signer repudiates a signature or made forged.

A general digital signature scheme is depicted as follows the document to be signed is and processed by a hash function in order to produce a genuine message digest, later that digest is signed using transmitter private key. The signed digest along with original document is transmitted to the receiver. At the receiver side, the signature legitimacy is verified and compared with the digest of the received message. ECDSA can be generated in the three different steps : Key pair generation, signature generation and the signature verification .It is based on three blocks private key generator, public key generator and SHA(secure hash algorithm) to obtain the condensation of message.

The result improvement security ECDSA 'S given by its hardware implementations. Hardware implementations are faster compare to software implemented solutions and are attractive for cryptosystems. Binary fields F2m with polynomial basis are better preferred for hardware implementations because some arithmetic operations are easier to compute. In this our proposed protocol is ECDSA recently this is recently used in smart cards and wireless devices and has wide applications that need low-bandwidth, low-storage and low-computation environments.

II. RELATED WORK AND CONTRIBUTIONS

With the advent of network technology, internet attacks are also versatile. So, the traditional encryption and decryption algorithms is not sufficient for securing the information over network. The alternative is to design an algorithm which will addresses the need of security with less effort. The digital signature algorithm process based on secured multilevel pseudo random generator that helps in obscuring key generation process. The ECDSA cryptosystem is develop provide to provide a shield against message attacks and the cryptosystem mainly concentrates on increased level of security, the Goldwasser-Micali algorithm haven been used for key generation process.

Lopez and Ahab pre a Montgomery multiplication for binary fields. The Diffie_hellman key exchange is implemented using the group of points on an elliptic curve over the field $F2^m$ .A software version of this using n=155 is optimized which achieves higher computation rates that are slightly faster than non-elliptic curve versions with same level of security.

The paper describes the implementations of cryptographic protocols, in which developed a simple version of the Diffie-

Hellaman protocol in transient modes,where the two parties select a random exponent e and exchange values of g^e ,where g is a group element.If party A selects e=a and party B selects e=b,then each party computes g^{ab} .They used the ring Zp with p a 512 bit prime,a size that should resists attacks with hardware resouces.The protocol took from 2 to 10 seconds on a variety of modern and hardware platforms.This has an advantage that as computer gets faster and the size of the numbers needed to achieve a particular level of security is much slowly for elliptic curve cryptosystems when compared to ordinary integers.The elliptic curve method uses a d group operation than multiplication of integers mod p.The size of the for group is approximately 2^{155} A.The group operation is implemented using Galois field F_2^{155} .Initial implementation was more than twice fast as computation using integer modulo a 512 bit prime. For the DH key exchange algorithm a properly chosen elliptic curve over F_2^{155} A is somewhat more security than a modulo a 512 bit prime.The improvements described here are how effectively compute the field operations in F^{255} especially for reciprocals which has a minor improvement can be used for doubling an elliptic curve point.The most important contribution of this is the fast recriprocal routine..As computing power increases and the search capabilities of opponents improve accordingly, it is better to improve the security of elliptic curve methods.The main contribution of this paper can be summarized as:

1. Special case code for squaring number which used to reduce the time to 60% of a multiplication.

2.The modulus is chosed as a prime in the form 2^{512} –K reduces the time for modular reduction to 10% of multiplication.

3.The base g to be exponentated ,the tables of g+-32^kS are prepared in advance.For a random 512 bit exponent this will reduce the reqired number of modular multiplications to 114 on average and eliminates squaring.[1]

Julio and Richardo described a binary field multiplications and ECC over binary field which mainly describes an algorithm for computing elliptic scalar multiplcations on non-singular elliptic curves defined over GF(2M). From the point of hardware implementation of elliptic curves over GF(2^m),few papers have discussed efficient methods for computing KP.However the formulas used for implementing each iteration are not efficient in terms of field multiplcations.The algorithm is used is optimized version of a method which is based on Montgomery ‘s method which is easy to implement in both hardware and software,requires no precomputed multiples of a point and it is faster on average than addition-subtraction method.This method requires less memory than projective coordinates and amount of computation needed for a scalar multiplication is fixed for all multipliers of same binary length. For a hardware implementation of GF (2^{155}) and software implementation of GF (2^{155}) and GF (2^{191}).In this paper, the calculation of KP for a random integer k and a random point P is considered was introduced by Montgomery based on the binary method and the observation the x-coordinates of the sum of two points whose difference is computed in x-coordinates of the involved points. This method maintains the invariant relationship P2-P1=P, and performs an addition and a doubling in each iteration. The Montgomery’s method is applied basically for reducing the number of registers which are needed to add points in super singular curves over GF(2M). The method performs exactly 6[log2k]+10 field multiplication for computing Kip on elliptic curves selected at random. The method appears for applications of elliptic curves in constraint environments such as mobile devices and smart cards..Implemented binary method in projective coordinates on averafe is 27-29% faster than addition-subtraction method and 51% faster than binary method[2].

E.Ozturk,B.Sunar proposed a new modulus scaling techniques fo transforming a class of primes into special forms which gives efficient arithemetic.The scaling technique which usually used to improve multiplication and inversion in finite fields and presented an efficient inversion algorithm that utilizes the structure of scaled modulus. Inversion algorithm exhibits the higher performance compare to the Euclidean algorithm and lends itself hardware implementation due its simplicity. By using modular techniques and specialized inversion algorithm develop an elliptic curve processor architecture. The successful use of redundant representation in all arithmetic operations which includes the inversion with the an comparator design leads to a significant reduction in critical path delay which results in very high operating clock frequency. It can be identified that same data path is used for all the field operations leads to a very small chip area. The architecture which will require extremely low power at very small footprint and provides high executable speed for elliptic curve implementation[3].

Cohen et al described the impact of coordinate system in ECC implementation. The results shows performance of point addition and point doubling of different coordinate system achieves the fastest doubling operations for binary operations curves. Berlekamp’s algorithm for multiplicative inverse and Montgomery‘s technique for modular multiplication. This paper describes a solution a binary add-and-shift algorithm for modular division . This technique is used for the fastest computation of divisions in GF(2m).An algorithm for calculating the modular inverse of an integer can be found by Aryabhatta.The extended Euclidean algorithm is adapted for computing the multiplicative inverse of binary polynomial over GF(2m).Berlekamp ‘s algorithm finds a polynomial r(t) of degree<m that satisfies r(t)p(t)=1 mod M(t) is the

multiplicative inverse of p(t) mod M(t).It can be improved by combining the iterations of the division and Euclid 's algorithm.Both can be combined into a unified procedure such that it doesn't require any division method, but only shift and addition operations. Montgomery introduced an reliable technique for multiplying integers modulo N which doesn't involve any division by M.Ths. algorithm provides an efficient technique for computing modular exponentiations and is used in RSA. The main contribution of this paper

1. Design of a field-division on elliptic curve crypto accelerator which uses simple iterative binary add-and-shift operations

2. Using iterative wide-registers and bit-parallel logic circuits that can perform an addition and shift in one cycle.

3. A hardware accelerator is built which dramatically enhance the efficiency of a cryptosystem[4]

G.N. Purohit described briefly the arithmetic operations focus on scalar multiplication which uses two different techniques by reducing hamming weight of scalars in binary representation and sliding window method are used. The main contribution of this paper Optimization for implementing ECC over binary fields which will improve the performance and viability .ECC based primitives such as key exchange or encryption is the scalar multiplication viewed as top level. The point scalar multiplication is successfully done by repeated point addition and doubling and modular and algorithms for modular exponentiation for point multiplication is used. The main contribution of this paper is it proposes a scalar multiplication which improves the computational efficiency of scalar multiplication. In sliding window a technique called windowing which is used by internet's transmission control protocol which will control the flow of packets between two computers or network hosts. It has accepted to support a wide variety of applications where ECC offers a proper solution to the problem which helps in implementing public key cryptography on mobile computing devices.The implementation of reducing the hamming weight and using sliding windows method reduces number of additions and doubling operations in scalar multiplication[5]

Jarvinen and skytta proposed a NIOS 2 based ECDSA implemented on an Altera Cyclone II FPGA. The ECDSA cryptosystem is develop provide to provide a shield against message attacks and the cryptosystem mainly focuses on increased level of security.Key features of ECDSA algorithms have been implemented successfully. .An architecture to implement Nios II processor t with designed modules for elliptic curve cryptography, SHA-1 hash function and modular arithmetic. A pseudo-random number generator is also included for rapid and secure generation of pseudo-random numbers to strengthen the cryptosystem. A user interface is designed with Nikos II integrated development (IDE).The. The user interface is written in C language and it is used with the Nios II IDE which supports 4 operations:

1. Generation of new identities.
2. Signed messages.
3. Verification of signatures.
4. Performance evaluation

The user interface uses host file system which will support IDE , it stores and handles messages and signatures on the host computer.The ECDSA functions directly control the peripheral components attached to Nios II .This include both top level function which performs high level tasks such as signature generation and verification and low level handles for controlling each component individual. These ECDSA functions are mainly used in real time applications.The developed cryptographic algorithm uses 163-B standardized curve performing key generation in 0.6ms,signature generation in 0.94ms and verification in 1.61ms.The design requires approximately 85% of the device resources.The key generation is expectedly the fastest operation than verification because it requires only one point multiplication and generation of random numbers whereas verification requires two point multiplications is expectedly the slowest operation.[6]

Michel hotter proposed the design of 192-bit ECDSA processor on Fp for RFID authentication only to signs a message within 859188 clock cycles is implemented RFID using microcontroller and with integrated AES(Advance Encryption standard) a challenge responsive protocol to allow tag and reader authentication. ECDSA could meet low-power requirements on RFIDs assuming clock frequency of 127ms at 6.78MHZ suggested frequency results in a reasonable performance for RFID applications while reducing power consumption.The paper presents a 192-bit elliptic curve digital signature algorithm process that allows entity and message authentication by digitally signing the challenges from the reader.The proposed architecture enhances the state of art in designing low resource ECDSA-enabled RFID.A tiny microcontroller used to provide protocol stability and re-use of common algorithms [7].

Glas proposed ECDSA signature processing system over prime fields for bit length 256 on reconfigurable hardware the performance can be improved to two orders of magnitude compared to microcontroller implementation. The flexible system is designed to serve as an autonomous subsystem provides authentication transparent for all application. Integration into a vehicle-to-vehicle communication system is shown as an example. The implementation results indicates signature generation in 7.15ms is expectedly the slowest operation requires a point multiplication and generation of a random integer. Verification in 9.09ms which requires computation of two point multiplications is expectedly the fastest operation[8]

L.Batina proposed the identification of RFID-tags will reach high security levels and identification protocols like RFID-tags based on the DL problem on elliptic curves are implemented on a constrained device which requires 8500 and 1400 gates. Case of both elliptic curved over F_2^P C and over composite fields F_2^2 P are investigated. This type of implementation made RFID tags suitable for anti-counterfeiting even in the offline setting.

The main contribution can be summarized as follows:

1).Feasibility of EC on RFID tags: ECC implementations of secure identification protocols such as scour's on a RFID-tags are presented and trading off performance for area is an important cost factor for the price of RFID-tags which minimizes the area which is required for implementations. This mainly focused on implementation of EC over binary fields which has an area complexity of between 12k and 15k equivalent gates. This area complexity which includes RAM and can be estimated upto 6 equivalent gates per RAM cell.

2) Trade off security for performance is acceptable: The smaller operand bit-lengths increases the efficiency of cryptographic operations like decryption, signature verification, etc..However this is not favoured in the crypto community because of the reduced security offered by resulting system. But however analysed the security that an EC over a field F_2^{131} C based on the current state of the art attacks and concluded that such fields offer admissible security for many RFID applications including anti-counterfeiting.

3). Solution based on identification schemes: Emphasize solution is based on identification schemes such as Scour because it provides additional way to save area. Challenge response protocol where an ECDSA signature is computed which requires the computation of hash, which requires significant hardware resources with 23,000 equivalent gates of their smallest EC processor design.

This work provides a evidence that ECC on RFID gives a viable solution in the near future.It allows more sophisticated protocols based pn public keys.Considered ECC over F2p operands between 130 and 140bits in length and composite fields. Different ALU configurations to obtain more compact and still accetsble performance are also shown.The design criteria which leads to low-power implementations to minimize the area and operating frequency[9]

CONCLUSION

This paper describes a comprehensive study of the strategies and recent development in Elliptical curve digital signatures which includes security of cryptosystem, RFID-aunthentication,Signature generation, Signature verification, scaling moduli in elliptical curve cryptography, Montgomery multiplication over binary field, point doubling and point addition of different coordinate system.

REFERENCES

[1] 1.R.Schroppel ,C. Beaver and O. Spatscheck "Fast key exchange With elliptic curve systems advances in cryptology-Crypto 95, Lncs 963, vol 43-56.

[2] 2. J.lopez and R.Ahab."Fast multiplication on elliptic curves over GF (2m) without precomputation in cryptographic hardware and embedded systems-CHES'99 Volume 1717 of lecture notes of computer science, pages 316-327, springer Verilog.

[3] E.Ozturk et al "Low-power elliptic curve cryptography using scaled modular arithmetic"—proc. 11th Ann. Int'l Cryptology Conf., IEEE, Pp. 279-287, 1992.

[4] COHEN ,H,MIYAJI,A,ANDONO,T."Efficient elliptic curve exponentiation using mixed coordinates, in proceedings of the international conference on the theory and applications of cryptology and information security,vol 51-65.

[5] G.N purohit "Efficient implementation of Arithmetic operations in ECC over Binary fields", International Journal of computer Application, vol 6-no.2,September 2010.

[6] K. J¨arvinen And J. Skytt¨a, "Crypto processor For Elliptic Curve Digital Signature Algorithm (ECDSA)," Tech. Rep., Helsinki University Of Technology, Signal Processing Laboratory, 2007

[7] Michael Hutter, Martin Feldhofer, And Thomas Plos"an Ecdsa Processor For RFID Authentication"Rfidsec ,IEEE transactions volume 6370, Pp. 189–202, 2010

[8] Benjamin Glas, Oliver Sander, Vitali Stuckert, Klaus D.Muller-glaser, And Jurgen Becker " Prime Field ECDSA Signature Processing For Reconfigurable Embedded Systems" International Journal Of Reconfigurable Computing Volume 2011

[9] L.Batina, J.Guajardo,T.Kerins,"An Elliptic curve processor suitable for RFID-tags",International Journal of Recofigurable Computing Volume 2008.